HIPAA Authorization Regulations

According to HIPAA requirements outlined in 164.508, researchers should obtain written authorization from subjects before using or collecting protected health information. Authorization should be obtained in writing from prospective subjects.*

Under HIPAA, the following core elements and statements must be included in the authorization document.

- A description that identifies the individually identifiable protected health information (PHI)** to be used/disclosed in a specific and meaningful fashion (e.g., list the types of data to be collected from the medical record);

- The name of the person(s) or class of persons to whom the covered entity may make the requested use or disclosure (i.e., researchers must list all of the entities that might have access to the study's PHI such as DCI/IRB, WRAMC, USUHS representatives, sponsors, Food and Drug Administration, data safety and monitoring board or any others given authority by law);

- A description for each purpose of the requested use or disclosure (e.g., list reasons why the PHI is collected such as to be able to conduct the research and to ensure that the research meets legal institutional or accreditation requirements, list purpose of research);

- An expiration date or an expiration event that relates to the use or disclosure (i.e., length of time researchers plan to maintain the data). The statement "end of research study", "none", or similar language is sufficient;

- A description of how the individual may revoke the authorization and the exceptions to the revocation; or a copy of the Privacy Notice which explains how to revoke the authorization and the exceptions to the revocation (i.e., HIPAA gives subjects the legal right to revoke authorization. The subject must be told how they can withdraw. Any request for revocation must be in writing. Also, the subjects should be told that if they do revoke, that they can no longer participate in research and that researchers may use the PHI already obtained to maintain the integrity of the data.);

- A statement that a subject's treatment, payment or enrollment in any health plan or their eligibility for benefits will not be effected if they refuse to sign the authorization;

- A statement that the subject may not participate in a research study if they refuse to sign the authorization;

---

* Currently at the WRAMC a researcher can obtain PHI without authorization only if the data (PHI) is de-identified or an IRB approved Waiver of Authorization is obtained.

**PHI: individually identifiable health information transmitted or maintained in any form (electronic means, on paper, or through oral communication) that relates to the past, present or future physical or mental health or conditions of an individual.

- An explanation that information disclosed pursuant to the authorization may no longer be protected when re-disclosed by the recipient (i.e., if the researchers disclose the information collected to a third party then the HIPAA protections may no longer be in place);
- A signature of the individual and date. If a personal representative signs the authorization, a description of the representative's authority must be provided;
- Optional item: Under HIPAA, subjects have the right to access their PHI. In research, this right can be suspended while the research is in progress. However, subjects must be told in the authorization that this right has been suspended and the conditions of the suspension must be listed. The subjects should also be informed that their right to access the PHI will be reinstated at the conclusion of the research study.
- The authorization must be written in plain language;
- The subject must be given a copy of the signed authorization.

What HIPAA Means To Researchers & IRBs

WHAT IS HIPAA?

HIPAA stands for the Health Insurance Portability & Accountability Act of 1996. HIPAA is also known as the Kennedy-Kassebaum Act.

HIPAA calls for:

1. Standardization of electronic patient health, administrative and financial data;
2. Unique identifier's for individuals, employers, health plans and health care providers;
3. Security standards protecting the confidentiality and integrity of health information.'

HIPAA & Privacy Rule:

The Privacy Rule for HIPAA was published on August 14, 2002 and the regulations effect researchers and IRBs. The Privacy Rule establishes privacy standards to protect a person's health information.

Privacy Standards:

- Limits the use and disclosure of health information;
- Gives patients the right to access their medical records and to receive an accounting of who accessed their health information;
- Allows patients to requests amendments to their medical records and place restrictions on uses and disclosures;
- Restricts most disclosures of health information to the minimum intended purpose;
- Establishes criminal and civil penalties for improper use or disclosure;
- Establishes new requirements for access to records by researchers.'

Penalties For Improper Disclosure:

The Privacy Rule restricts disclosure of health information for specific purposes and establishes criminal and civil penalties for improper disclosure and/or use. Fines can go as high as:

- **$25,000** for multiple violations in the same year;
- **$250,000 and/or up to 10 years imprisonment** for knowingly misusing a person's protected health information.

Compliance Date:

The Privacy Rule becomes effective on April 14, 2003; however, federal regulations allow an additional year for business associates contracts, a contract where one party performs a function or activity involving the use of protected health information (PHI). Business associate contracts must meet the HIPAA requirements before April 14, 2004.

HOW DO RESEARCHERS ACCESS PATIENT INFORMATION?

Researchers who want access to protected health information (PHI) must request the information from and meet the requirements of the covered entity, which in this case is The Military Health Care System. The Privacy Rule allows for the PHI information to be released if the request meets one of the following six conditions:

1. A patient authorization is obtained;
2. Authorization requirement is waived by IRB/Privacy Board;
3. Information is collected only for preparatory work for research;
4. Only a limited data set is collected and accompanied with a data use agreement;
5. Only decedent PHI is being collected;
6. Information requested is "de-identified."

Each of these six conditions is discussed below.

1. Accessing Information through Patient Authorization (Section 164.508)

A researcher may use or disclose protected health information with a valid authorization. A valid authorization must have the following elements:

A. Core Elements and Required Statements

- A description that identifies the information in a specific and meaningful fashion; and
- The name of the person(s) authorized to make the requested use or disclosure; and
- The name of the person(s) to whom the covered entity may make the requested use or disclosure; and
- A description for every requested use or disclosure; and
- An expiration date or an expiration event that relates to the use or disclosure. The statement "end of the research study," "none," or similar language is sufficient if the authorization is research; and
- A description of how the individual may revoke the authorization and the exceptions to the revocation; or a copy of the Privacy Notice which explains how to revoke the authorization and the exceptions to the revocation; and

  Statement that a subject's treatment, payment or enrollment in any health plan or their eligibility for benefits will not be effected if they refused to sign the authorization; and
- The subject may not participate in a research study if they refuse to sign the authorization; and

- Explanation that information disclosed for the authorization may no longer be protected when redisclosed by the recipient.
- Signature of the individual and date. If a personal representative signs the authorization, a description of the representative's authority must be provided.

B. Additional Authorization Requirements

- The authorization must be written in plain language.
- The subject must be given a copy of the signed authorization.

C. Combining the Authorization with the Consent Form

- The revised Privacy Rule allows an authorization to be combined with a research consent form.

D. Research Uses/Disclosures Where An Authorization Is Not Required (164.512)

FDA-regulated research does NOT require an authorization for the following activities:

•Collecting and reporting adverse events; or

- Tracking FDA-regulated products; or
- Enabling product recalls, repairs, replacement, and look-backs; or
- Conducting post marketing surveillance;

2. Accessing Information Through A Privacy Board/IRB Approved Waiver (Section 164.12)

A researcher may access PHI though a wavier but the waiver must satisfy the following criteria:

A. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals; and

B. The use or disclosure must include a plan to protect PHI from improper use/disclosure; and

C. The use or disclosure must include a plan to destroy PHI at the earliest opportunity unless there is justification for retaining the information; and

D. The researcher must submit written assurances that PHI will not be reused or disclosed to 3rd parties unless required by the research study or law enforcement agencies; and

E. The research could not practicably be conducted without the waiver; and

F. The research could not practicably be conducted without access to and use of PHI.

3. Accessing Information for Preparatory Work for Research (Section 164.512)

A researcher may review PHI for preparatory work for research without an authorization. In order to view PHI, the researcher must submit a request to the entity documenting that:

- Reviewing protected health information is necessary to prepare a research protocol; and
- Information will not be removed by the researcher during the review; and
- The information is necessary for research purposes.

4. Accessing Information through Limited Data Sets (Section 164.514)

A. A covered entity may use or disclose a limited data set only if the covered entity obtains satisfactory assurance, in the form of a data use agreement, that the information will only be:

- Used for research, public health, or health care operations;
- Disclosed to business associates;
- Used/disclosed for limited purposes by the recipient.

B. A limited data set is protected health information that excludes the following direct identifiers:

1. Names;
2. Postal address information, other than town or city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

C. Data use agreements must:

1. Establish the permitted uses and disclosures by the recipient;
2. Establish who is permitted to use or receive the limited data set; and
3. Provide that the limited data set recipient will:

- Not use/disclose the information other than as permitted by the data use agreement or required by law;

- Use appropriate safeguards to prevent use/disclosure other than as provided for by the data use agreement;
- Report to the covered entity any use/disclosure not stated in the data use agreement;
- Ensure that any agents, including subcontractors, agrees to the same restrictions and conditions that apply to the limited data set recipient; and
- Not identify the information or contact the individuals.

5. Accessing Information on Deceased Persons (Section 164.512)

A researcher may review PHI from deceased persons without authorization. For this information, the researcher must submit a request to the entity stating that:

- The use/disclosure of PHI is for research purposes only; and
- The information is necessary for research purposes; and
- The person is deceased and providing documentation that the person is deceased.

6. Accessing Information though De-identification (Section 164.514)

De-identified health information may be released without an authorization and exempts the release from HIPAA requirements. De-identification is defined as health information that does not contain any information that allows a researcher to identify a person. A covered entity may de-identify PHI only if:

A. A statistician, or other qualified expert, de-identifies PHI through generally accepted statistical and scientific methods and determines that:

- The risk of re-identifying the information is very small; and
- Documents the methods and results of the analysis that justify such determination; or

B. De-identifying PHI by removing all of the 18 identifiers listed below:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes;
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;

13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code.

C. To release **any** information without a patient authorization, the entity cannot have actual knowledge that the de-identified information could be used to identify an individual.

D. A covered entity may assign a code to allow re-identification of PHI, provided that:

- The code or other means of record identification is not derived from or related to information about the individual and can not be used to identify the individual; and
- The entity does not use/disclose the code for any other purpose; and
- The covered entity does not disclose the re-identification code.

Please note that de-identification only satisfies the HIPAA requirements and not the IRB requirements.

ADDITIONAL INFORMATION THAT RESEARCHERS SHOULD KNOW

HIPAA also affects the following areas:

Specimens And Tissue Samples. Which Include PHI:

Research involving specimens and tissues that include accompanying PHI are covered under H I PAA.

Business Associate Contracts (Section 164.504

A business associate contract is a contract between 2 parties where one party performs a function or activity involving the use or disclosure of PHI.

Accounting of Disclosures (Section 164.528):

The Privacy Rule allows an individual the right to receive an accounting of disclosures of PHI made by an entity with the exception of certain disclosures.

Minimum Use Disclosures (Section 165.514):

An entity must limit the amount of PHI disclosed to recipients to the "minimum necessary."

HIPAA & IRB Human Protection Regulations:

HIPAA does not override IRB requirements. When HIPAA and human subject protection regulations apply, both sets of requirements must be followed.

What is the Common Rule?

The Department of Health & Human Services Code of Federal Regulations (45CFR-46) entitled "Human Subjects Protection" is also known as "The Common Rule". Specifically, Subpart-A of this regulation is referred as the Common Rule because it was adopted as the rule in human research b 17 federal agencies.

The Common Rule is what governs the Institutional Review Board (IRB; at WRAMC it is known as the Human Use Committee, HUC) and the implementation of the responsible conduct of research.

RESEARCH

Frequently Asked Questions

Q: Will the HIPAA Privacy Rule hinder medical research by making doctors and others less willing and/or able to share with researchers information about individual patients?

A. We do not believe that the Privacy Rule will hinder medical research. Indeed, patients and health plan members should be more willing to authorize disclosures of their information for research and to participate in research when they know their information is protected. For example, in genetic studies conducted at the National Institutes of Health, nearly 32 percent of eligible people offered a test for breast cancer risk declined to take it. The overwhelming majority of those who refuse cite concerns about health insurance discrimination and loss of privacy as the reason. The Privacy Rule both permits important research and, at the same time, encourages patients to participate in research by providing much needed assurances about the privacy of their health information.

The Privacy Rule will require some covered health care providers and health plans to change their current practices related to documenting research uses and disclosures. It is possible that some covered health care providers and health plans may conclude that the Rule's requirements for research uses and disclosures are too burdensome and will choose to limit researchers' access to protected health information. We believe few providers will take this route, however, because the Common Rule includes similar, and more rigorous requirements, that have not impaired the willingness of researchers to undertake Federally-funded research. For example, unlike the Privacy Rule, the Common Rule requires an Institutional Review Board (IRB) review for all research proposals under its purview, even if informed consent is to be sought. The Privacy Rule requires documentation of IRB or Privacy Board approval only if patient authorization for the use or disclosure of protected health information for research purposes is to be altered or waived. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.

Q: Are some of the criteria so subjective that inconsistent determinations may be made by Institutional Review Boards (IRB) and Privacy Boards reviewing similar or identical research projects?

A: Under the HIPAA Privacy Rule, IRBs and Privacy Boards need to use their judgment as to whether the waiver criteria have been satisfied. Several of the waiver criteria are closely modeled on the Common Rule's criteria for the waiver of informed consent and

for the approval of a research study. Thus, it is anticipated that IRBs already have experience in making the necessarily subjective assessments of risks. While IRBs or Privacy Boards may reach different determinations, the assessment of the waiver criteria through this deliberative process is a crucial element in the current system of safeguarding research participants' privacy. The entire system of local IRBs is, in fact, predicated on a deliberative process that permits local IRB autonomy. The Privacy Rule builds upon this principle; it does not change it. Nonetheless, the Department will consider issuing guidance as necessary and appropriate to address concerns that may arise during implementation of these provisions. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule and Institutional Review and Privacy Boards.

Q: Does the HIPAA Privacy Rule prohibit researchers from conditioning participation in a clinical trial on an authorization to use/disclose existing protected health information?

A: No. The Privacy Rule does not address conditions for enrollment in a research study. Therefore, the Privacy Rule in no way prohibits researchers from conditioning enrollment in a research study on the execution of an authorization for the use of pre-existing health information.

Q: Does the HIPAA Privacy Rule permit the creation of a database for research purposes through an Institutional Review Board (IRB) or Privacy Board waiver of individual authorization?

A: Yes. A covered entity may use or disclose protected health information without individuals' authorizations for the creation of a research database, provided the covered entity obtains documentation that an IRB or Privacy Board has determined that the specified waiver criteria were satisfied. Protected health information maintained by a covered entity in such a research database could be used or disclosed for future research studies as permitted by the Privacy Rule – that is, for future studies in which individual authorization has been obtained or where the Rule would permit research without an authorization, such as pursuant to an IRB or Privacy Board waiver. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: Can researchers continue to access existing databanks or repositories that are maintained by covered entities, even if those databases were created prior to the compliance date without patient permission or without a waiver of informed consent by an Institutional Review Board (IRB)?

A: Yes. Under the HIPAA Privacy Rule, covered entities may use or disclose protected

health information from existing databases or repositories for research purposes either with individual authorization as required at 45 CFR 164.508, or with a waiver of individual authorization as permitted at 45 CFR 164.512(i). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review Boards.

Q: How does the Rule help Institutional Review Boards (IRB) handle the additional responsibilities imposed by the HIPAA Privacy Rule?

A: Recognizing that some institutions may not have IRBs, or that some IRBs may not have the expertise needed to review research that requires consideration of risks to privacy, the Privacy Rule permits the covered entity to accept documentation of waiver of authorization from an alternative body called a Privacy Board–which could have fewer members, and members with different expertise than IRBs. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

In addition, the Rule allows an IRB to use expedited review procedures as permitted by the Common Rule to review and approve requests for waiver of authorizations. Similarly, the Rule permits Privacy Boards to use an expedited review process when the research involves no more than a minimal privacy risk to the individuals. An expedited review process permits covered entities to accept documentation of waiver of authorization when only one or more members of the IRB or Privacy Board have conducted the review. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.

Q: By establishing new waiver criteria and authorization requirements, hasn't the HIPAA Privacy Rule, in effect, modified the Common Rule?

A: No. Where both the Privacy Rule and the Common Rule apply, both regulations must be followed. The Privacy Rule regulates only the content and conditions of the documentation that covered entities must obtain before using or disclosing protected health information for research purposes. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule.

Q: Is documentation of Institutional Review Board (IRB) *and* Privacy Board approval required by the HIPAA Privacy Rule before a covered entity would be permitted to disclose protected health information for research purposes without an individual's authorization?

A: No. The HIPAA Privacy Rule requires documentation of waiver approval by either an

IRB *or* a Privacy Board, not both. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: Does the HIPAA Privacy Rule require a covered entity to create an Institutional Review Board (IRB) or Privacy Board before using or disclosing protected health information for research?

A: No. The IRB or Privacy Board could be created by the covered entity or the recipient researcher, or it could be an independent board. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: What does the HIPAA Privacy Rule say about a research participant's right of access to research records or results?

A: With few exceptions, the Privacy Rule gives patients the right to inspect and obtain a copy of health information about themselves that is maintained by a covered entity or its business associate in a "designated record set." A designated record set is basically a group of records which a covered entity uses to make decisions about individuals, and includes a health care provider's medical records and billing records, and a health plan's enrollment, payment, claims adjudication, and case or medical management record systems. While it may be unlikely that a researcher would be maintaining a designated record set, any research records or results that are actually maintained by the covered entity as part of a designated record set would be accessible to research participants unless one of the Privacy Rule's permitted exceptions applies.

One of the permitted exceptions applies to protected health information created or obtained by a covered health care provider/researcher for a clinical trial. The Privacy Rule permits the individual's access rights in these cases to be suspended *while the clinical trial is in progress*, provided the research participant agreed to this denial of access when consenting to participate in the clinical trial. In addition, the health care provider/researcher must inform the research participant that the right to access protected health information will be reinstated at the conclusion of the clinical trial.

Q: Are the HIPAA Privacy Rule's requirements regarding patient access in harmony with the Clinical Laboratory Improvements Amendments of 1988 (CLIA)?

A: Yes. The Privacy Rule does not require clinical laboratories that are also covered health care providers to provide an individual access to information if CLIA prohibits them from doing so. CLIA permits clinical laboratories to provide clinical laboratory test records

and reports only to "authorized persons," as defined primarily by State law. The individual who is the subject of the information is not always included as an authorized person. Therefore, the Privacy Rule includes an exception to individuals' general right to access protected health information about themselves if providing an individual such access would be in conflict with CLIA.

In addition, for certain research laboratories that are exempt from the CLIA regulations, the Privacy Rule does not require such research laboratories, if they are also a covered health care provider, to provide individuals with access to protected health information because doing so may result in the research laboratory losing its CLIA exemption.

Q: Do the HIPAA Privacy Rule's requirements for authorization and the Common Rule's requirements for informed consent differ?

A: Yes. Under the Privacy Rule, a patient's authorization is for the use and disclosure of protected health information for research purposes. In contrast, an individual's informed consent, as required by the Common Rule and the Food and Drug Administration's (FDA) human subjects regulations, is a consent to participate in the research study as a whole, not simply a consent for the research use or disclosure of protected health information. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about the Common Rule. For this reason, there are important differences between the Privacy Rule's requirements for individual authorization, and the Common Rule's and FDA's requirements for informed consent. However, the Privacy Rule's authorization elements are compatible with the Common Rule's informed consent elements. Thus, both sets of requirements can be met by use of a single, combined form, which is permitted by the Privacy Rule. For example, the Privacy Rule allows the research authorization to state that the authorization will be valid until the conclusion of the research study, or to state that the authorization will not have an expiration date or event. This is compatible with the Common Rule's requirement for an explanation of the expected duration of the research subject's participation in the study. It should be noted that where the Privacy Rule, the Common Rule, and/or FDA's human subjects regulations are applicable, each of the applicable regulations will need to be followed.

Q: When is a researcher a covered health care provider under HIPAA?

A: A researcher is a covered health care provider if he or she furnishes health care services to individuals, including the subjects of research, and transmits any health information in electronic form in connection with a transaction covered by the Transactions Rule. See 45 CFR 160.102, 160.103. For example, a researcher who conducts a clinical trial that involves the delivery of routine health care, such as an MRI or liver function test, and

transmits health information in electronic form to a third party payer for payment, would be a covered health care provider under the Privacy Rule. Researchers who provide health care to the subjects of research or other individuals would be covered health care providers even if they do not themselves electronically transmit information in connection with a HIPAA transaction, but have other entities, such as a hospital or billing service, conduct such electronic transactions on their behalf. For further assistance in determining covered entity status, see the "decision tool" at www.hhs.gov/ocr/hipaa/.

Q: When does a covered entity have discretion to determine whether a research component of the entity is part of their covered functions, and therefore, subject to the HIPAA Privacy Rule?

A: A covered entity that qualifies as a hybrid entity, meaning that the entity is a single legal entity that performs both covered and non-covered functions, may choose whether it wants to be a hybrid entity. If such a covered entity decides not to be a hybrid entity then it, and all of its components, are subject to the Privacy Rule in its entirety. Therefore, if a researcher is an employee or workforce member of a covered entity that has decided not to be a hybrid entity, the researcher is part of the covered entity and is, therefore, subject to the Privacy Rule.

If a covered entity decides to be a hybrid entity, it must define and designate as its health care component(s) those parts of the entity that engage in covered functions. "Covered functions" are those functions of a covered entity that make the entity a health plan, a health care provider, or a health care clearinghouse. Thus, research components of a hybrid entity that function as health care providers and engage in standard electronic transactions must be included in the hybrid entity's health care component(s), and be subject to the Privacy Rule.

However, research components that function as health care providers, but do not engage in standard electronic transactions may, but are not required to, be included in the health care component(s) of the hybrid entity. For example, a hybrid entity, such as a university, has the option to include or exclude a research laboratory, that functions as a health care provider but does not engage in electronic transactions, as part of the hybrid entity's health care component. If such a research laboratory is included in the hybrid entity's health care component, then the employees or workforce members of the laboratory must comply with the Privacy Rule. But if the research laboratory is excluded from the hybrid entity's health care component, the employees or workforce members of the laboratory are not subject to the Privacy Rule.

Q: If a research subject revokes his or her authorization to have protected health information used or disclosed for research, does the HIPAA Privacy Rule permit a

researcher/covered health care provider to continue using the protected health information already obtained prior to the time the individual revoked his or her authorization?

A: Covered entities may continue to use and disclose protected health information that was obtained prior to the time the individual revoked his or her authorization, as necessary to maintain the integrity of the research study. An individual may not revoke an authorization to the extent the covered entity has acted in reliance on the authorization. For research uses and disclosures, this reliance exception at 45 CFR 164.508(b)(5)(i) permits the continued use and disclosure of protected health information already obtained pursuant to a valid authorization to the extent necessary to preserve the integrity of the research study. For example, the reliance exception would permit the continued use and disclosure of protected health information to account for a subject's withdrawal from the research study, as necessary to incorporate the information as part of a marketing application submitted to the Food and Drug Administration, to conduct investigations of scientific misconduct, or to report adverse events.

However, the reliance exception would not permit a covered entity to continue disclosing additional protected health information to a researcher or to use for its own research purposes information not already gathered at the time an individual withdraws his or her authorization.

Q: Can the preparatory research provision of the HIPAA Privacy Rule at 45 CFR 164.512(i)(1)(ii) be used to recruit individuals into a research study?

A: The preparatory research provision permits covered entities to use or disclose protected health information for purposes preparatory to research, such as to aid study recruitment. However, the provision at 45 CFR 164.512(i)(1)(ii) does not permit the researcher to remove protected health information from the covered entity's site. As such, a researcher who is an employee or a member of the covered entity's workforce could use protected health information to contact prospective research subjects. The preparatory research provision would allow such a researcher to identify prospective research participants for purposes of seeking their authorization to use or disclose protected health information for a research study. In addition, the Rule permits a covered entity to disclose protected health information to the individual who is the subject of the information. See 45 CFR 164.502(a)(1)(i). Therefore, covered health care providers and patients may continue to discuss the option of enrolling in a clinical trial without patient authorization, and without an Institutional Review Board (IRB) or Privacy Board waiver of the authorization. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.
However, a researcher who is not a part of the covered entity may not use the preparatory

research provision to contact prospective research subjects. Rather, the outside researcher could obtain contact information through a partial waiver of individual authorization by an IRB or Privacy Board as permitted at 45 CFR164.512(i)(1)(i). The IRB or Privacy Board waiver of authorization permits the partial waiver of authorization for the purposes of allowing a researcher to obtain protected health information as necessary to recruit potential research subjects. For example, even if an IRB does not waive informed consent and individual authorization for the study itself, it may waive such authorization to permit the disclosure of protected health information as necessary for the researcher to be able to contact and recruit individuals into the study.

Q: **Does the HIPAA Privacy Rule require documentation of Institutional Review Board (IRB) or Privacy Board approval of an alteration or waiver of individual authorization before a covered entity may use or disclose protected health information for any of the following provisions: (1) for preparatory research at 45 CFR 164.512(i)(1)(ii), (2) for research on the protected health information of decedents at 45 CFR 164.512(i)(1)(iii), or (3) a limited data set with a data use agreement as stipulated at 45 CFR 164.514(e)?**

A: No. Documentation of IRB or Privacy Board approval of an alteration or waiver of individual authorization is only needed before a covered entity may use or disclose protected health information under 45 CFR 164.512(i)(1)(i). See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review and Privacy Boards.

Q: **If research subjects' consent was obtained before the compliance date, but the Institutional Review Board (IRB) subsequently modifies the informed consent document after the compliance date and requires that subjects be reconsented, is authorization now required from these previously enrolled research subjects under the HIPAA Privacy Rule?**

A: Yes. If informed consent or reconsent (ie., asked to sign a revised consent or another informed consent) is obtained from research subjects after the compliance date, the covered entity must obtain individual authorization as required at 45 CFR 164.508 for the use or disclosure of protected health information once the consent obtained before the compliance date is no longer valid for the research. The revised informed consent document may be combined with the authorization elements required by 45 CFR 164.508. See the fact sheet and frequently asked questions about the research provisions on this web site for more information about Institutional Review Boards.

Q: **Can covered entities continue to disclose adverse event reports that contain protected health information to the Department of Health and Human Services**

(HHS) Office for Human Research Protections?

A: Yes. The Office for Human Research Protections is a public health authority under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to report adverse events to the Office for Human Research Protections either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for public health activities as permitted at 45 CFR 164.512(b).

Q: Can covered entities continue to disclose protected health information to the HHS Office for Human Research Protections for purposes of determining compliance with the HHS regulations for the protection of human subjects (45 CFR Part 46)?

A.: Yes. The Office for Human Research Protections is a health oversight agency under the HIPAA Privacy Rule. Therefore, covered entities can continue to disclose protected health information to the Office for Human Research Protections for such compliance investigations either with patient authorization as provided at 45 CFR 164.508, or without patient authorization for health oversight activities as permitted at 45 CFR 164.512(d).

HIPAA PRIVACY RULE
RESOURCES AND CONTACTS

NON-GOVERNMENTAL ORGANIZATIONS:

http://www.aamc.org/	Association of American Medical Colleges
http://www.aha.org	American Hospital Association
http://www.healthprivacy.org/	Health Privacy Project (sponsored by the Institute for Health Care Research and Policy, Georgetown University)
http://www.jhita.org/	Joint Healthcare Technology Alliance
http://www.mahealthdata.org/	Massachusetts Health Data Consortium (provides information on HIPAA compliance, Massachusetts Privacy Officers Forum, and links to other key HIPAA web sites)
http://www.hipaadvisory.com/	Phoenix Healthcare Systems (information on HIPAA compliance)
http://www.primr.org/about.html	Public Responsibility in Medicine and Research
http://www.wedi.org/	Workgroup for Electronic Data Exchange (a broad-based industry association which advises DHHS regarding EDI standards. Web site includes conference information, and health care EDI information)

FEDERAL AGENCIES:

http://www.hhs.gov	Department of Health and Human Services
http://aspe.hhs.gov/admnsimp	Administrative Simplification
http://cms.hhs.gov/hipaa/	Centers for Medicare and Medicaid Services
http://www.fda.gov	FDA home page
http://www.ncvhs.hhs.gov/	National Committee on Vital and Health Statistics
http://www.nih.gov	NIH home page
http://www.hhs.gov/ocr/hipaa/	Office for Civil Rights
http://ohrp.osophs.dhhs.gov/	Office for Human Research Protection
http://ori.hhs.gov	Office of Research Integrity

HIPAA Research Roadmap*

Are you intending to collect data on any of the 18 personal health identifiers? 1. Names 2. Street address, city, county, 5-digit zip code 3. Months and dates (years are OK) and ages >89 (unless all persons over 89 years are aggregated into a single category) 4. Telephone numbers 5. Fax numbers 6. E-mail addresses 7. Social security number 8. Medical record number 9. Health plan beneficiary number 10. Account number 11. Certificate/license number 12. Vehicle serial number or license plate number 13. Device identifiers and serial numbers 14. URLs (Uniform Resource Locators) 15. Internet protocol address number 16. Biometric identifiers, such as finger and voice prints 17. Full face photographic images or any comparable images 18. Any other unique identifying number, characteristic, or code such as patient initials	→	If No, HIPAA does not apply.
↓ Yes		
Can you limit your collection of protected health information (PHI) to just dates (#3 above), city/state/zip, or "other unique identifier" (#18 above)? (defined as a "limited data set" in HIPAA-speak)	→	If yes, include Data Use Agreement in protocol, to avoid the patient Authorization requirement
↓ No		
Do any of the 3 following HIPAA exceptions apply? 1. The research information has been de-identified:		If yes:
a. The dataset has been stripped of all 18 identifiers, or b. A statistician can document that there is less than a "very small" risk that an individual's identity can be detected.	→	A Waiver can be requested, or no patient Authorization may be necessary.
2. Obtaining patient Authorization is not "practicable" (protocol may qualify as "HIPAA minimum risk").	→	Request Waiver in protocol (remember that disclosure of PHI must be tracked).
3. Data collection is "preparatory to research" in order to determine how many/whether potential research subjects meet study recruitment criteria.	→	No Authorization necessary
↓ No		
Research subject will need to sign Authorization – the Authorization should be separate from the informed consent form		
↓		
Will any of the PHI be disclosed to persons outside the Military Health System? Non-MHS groups include: USUHS, NIH, MRMC, WRAIR, AFIP, universities, study sponsors, cooperative oncology groups, data coordinating centers, external tissue banks, etc.	→	If Yes, then a Business Associate Agreement is necessary (only if the entity is outside the DoD).

* Note: HIPAA is a complex law, and its research application is still subject to interpretation. This Roadmap is subject to revision as the interpretation of the law evolves. February 11, 2003